

# Safety-Critical, Real-Time, Embedded, Fault-Tolerant CORBA

Gary Daugherty, Rockwell Collins, [gwdaughe@collins.rockwell.com](mailto:gwdaughe@collins.rockwell.com)

We are interested in a Safety-Critical, Real-Time, Embedded, Fault-Tolerant version of CORBA for use in avionics systems. This, however, poses a number of difficulties. The current Real-Time and Fault-Tolerant CORBA standards conflict with one another in a number of important ways. For example, the execution times for the strategies used to implement fault-tolerance may result in unpredictable and unbounded execution times, which are unacceptable for Real-Time. The resource limitations of embedded systems similarly make it difficult to use Minimum CORBA for Real-Time and Fault-Tolerant applications. And none of these flavors of CORBA address concerns related to safety and certification issues such as:

- Failure to conform to FAA/NASA OO guidelines for DO-178B certification
- Failure to conform to language specific guidelines for safety critical systems
- Unrestricted use of dynamic allocation after initialization
- Use of unbounded data structures
- Use of algorithms with unpredictable or unbounded execution times
- Use of recursion
- Dynamic loading of classes
- Unrestricted use of exceptions
- Use of aliasing, involving pointers or arguments
- Choice of model for threads, synchronization and thread communication
- Potential for deadlock or starvation of threads within the ORB
- ORB size and complexity
- Lack of precise requirement specifications
- Lack of design documentation
- Lack of reliability

To be acceptable for use by most avionics applications, we must also be concerned with:

- Performance
- Footprint
- Data transfer rate
- Resource requirements
- Maintenance of a niche implementation (open-source or otherwise)

This leaves us in a quandary. Commercial products developed to OMG standards fall short because support for one market nice (e.g., Real-Time) often precludes support for another (e.g., Fault-Tolerance), when what we need is an intersection of solutions appropriate for both domains. As we attempt to deal with additional domains, however, the problem only becomes worse. What we need is a way to represent alternative solutions to the key problems in each domain in a manner that allows us to compose a system where the intersection of these solutions (e.g., for a Safety-Critical, Real-Time, Embedded, Fault-Tolerant) is not empty – i.e. allowing us to construct the kind of custom systems that we need at reasonable cost.

## References

Gary Daugherty. *Certifiability of CORBA*, Rockwell Collins Advanced Technology Center Technical Report, September 2001.

Object Management Group. *Rockwell Collins Response to Safety Critical RFI*, mars/02-03-01, available from the OMG web site ([www.omg.org](http://www.omg.org)).